

## **REMARKS**

The Office Action dated November 30, 2005, has been received and carefully noted. The above amendments to the specification, and the following remarks, are submitted as a full and complete response thereto. Claims 1-48 are submitted for consideration.

The specification was objected to because certain acronyms were not properly defined. The specification has been amended to define each of the acronyms. Therefore, Applicant requests that this objection be withdrawn.

According to the Office Action, the limitation “a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method” as recited in claims 1, 31, and 40 has been described insufficiently in paragraph 0069 of the specification. Applicant submits that paragraph 0069 discloses that figures 7-12 show different embodiments of the invention where the combinations of phases I and II depend on the protocols and authentication methods used in the illustrated embodiments. Thus, the limitation “a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method” as recited in claims 1, 31, and 40 has been described sufficiently in paragraph 0069 of the specification and the associated drawings.

Claims 1-48 stand rejected under 35 U.S.C. § 103(a) as allegedly being anticipated by U.S. Patent Publication No. 2002/0174335 (Zhang) in view of U.S. Patent Applicant

Publication 20030226017 A1 (Palekar). The Office Action alleges that Zhang teaches all the elements of claims 1-48 except for establishing a secure tunnel is determined based on a protocol or an authentication method. Thus, the Office Action combines the teachings of Zhang with Palekar to yield all elements of the presently pending claims. The rejection is traversed as being based on a reference that neither teaches nor suggests the novel combination of features clearly recited in independent claims 1, 31 and 40.

Claim 1, upon which claims 2-30 depend, recites in a communication system including at least one network, including network entities which provide connectivity to user equipment, a method of connecting the user equipment to the at least one network includes establishing a secure tunnel which provides connection between the user equipment and one of the network entities. The method also includes authenticating the user equipment with another of the network entities. The authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method.

Claim 31, upon which claims 32-39 depend, recites a communication system including at least one network, including network entities which provide connectivity to the user equipment. A secure tunnel is established which provides connection between the user equipment and one of the network entities. The user equipment is authenticated with another of the network entities. The authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the

establishing of the secure tunnel. The phase is determined based on protocol or authentication method.

Claim 40, upon which claims 41-48 depend, recites a user equipment in a communication system including at least one network, including network entities which provide connectivity to the user equipment. A secure tunnel is established which provides connection between the user equipment and one of the network entities. The user equipment is authenticated with another of the network entities, and the authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method.

As will be discussed below, the cited prior art references of Zhang and Palekar fails to disclose or suggest the elements of any of the presently pending claims.

Zhang relates to an IP-based authentication, accounting and authorization scheme for wireless local area network (LAN) virtual operators. Zhang describes mobile users accessing the internet and local network services at hot spots, such as airports, hotels or coffee shops. The internet service providers of the mobile users are used as the single point of contact for all authentication, accounting and authorization (AAA) transactions. Referring to Figure 1 of Zhang, a mobile terminal 110 communicates with a wireless LAN access point 120. Zhang describes access point 120 controlling the authentication by mobile terminal 110. Figure 2 of Zhang shows access point 120 assigning mobile terminal 110 a dynamic IP address. The user initiates a login session with the ISP. The

ISP id and the user id are sent to access point 120. Access point 120 sends the user's authentication server an access-request packet 210 with the user id. RSP 150' makes a validity determination with respect to the user id contained in the access-request packet 210. Zhang describes a filtering function installed on every access point 120 to filter all mobile traffic and determine whether the traffic should be let through or blocked. IPSEC is used between access points and mobile terminals for per-packet authentication or per-packet encryption. A packet filtering function employed at an access point serves as a transparent mechanism for controlling not only authentication and authorization, but also packet level accounting. With a mutual proof mechanism, Zhang describes avoiding potential accounting disputes without requiring all mobile traffic to go through a central entity.

Palekar discloses that a Transport Layer Security (TLS) protocol provides a mechanism for encrypting messages between two end points. The messages protected with the TLS protocol are to be transmitted through a TLS tunnel that was previously established. See paragraph 0008

Applicant submits that combination of Zhang and Palekar simply does not teach or suggest the combination of features clearly recited in claims 1-48. Each of claims 1, 31 and 40 recites, in part, authenticating of the user equipment with another of the network entities occurs **at least partially simultaneously with a phase of the establishing of the secure tunnel**, wherein the phase is determined based on a protocol or authentication method. Zhang fails to disclose or suggest the authenticating of the user equipment

occurring at least partially simultaneously with a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method as recited in claims 1, 31 and 40. Paragraph 0071 of Zhang teaches that when a mobile terminal moves into the coverage area of an access point, the mobile terminal first establishes a layer 2 connection with the access point. Thereafter, according to paragraphs 0073-0086 of Zhang, the authentication of the user is performed. Thus, Zhang fails to disclose or suggest the authenticating of the user equipment occurring at least partially simultaneously with a phase of the establishing of the secure tunnel as alleged by the Office Action and recited in the present claims.

Palekar does not cure the deficiencies of Zhang. Specifically, Palekar does not teach or suggest authenticating of the user equipment occurring at least partially simultaneously with a phase of the establishing of the secure tunnel, as recited in claims 1, 31 and 40. Furthermore, the Office Action alleged that although Zhang does not teach or suggest that the phase may be determined based on a protocol or authentication method, as recited in the present claims, Palekar teaches this element. As noted above, paragraph 0008 of Palekar teaches that the tunnels are established before authentication begins. Although Palekar discloses different methods of implementing the TLS protocol, Palekar teaches that the protocol is implemented after the tunnel is established. Thus, Applicant submits that Palekar teaches away from the elements recited in the present claims. Applicant submits that both Zhang and Palekar fail to disclose or suggest the authenticating of the user equipment occurring at least partially simultaneously with a

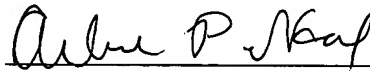
phase of the establishing of the secure tunnel, wherein the phase may be determined based on a protocol or authentication method as recited in the present invention. Thus, Applicant respectfully asserts that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Zhang nor Palekar, whether taken singly or combined, teaches or suggests each feature of claims 1, 31 and 40 and hence, dependent claims 2-30, 32-39 and 41-48 thereon.

As noted previously, claims 1-48 recite subject matter which is neither disclosed nor suggested in the prior art references cited in the Office Action. It is therefore respectfully requested that all of claims 1-48 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Arlene P. Neal

Registration No. 43,828

**Customer No. 32294**

SQUIRE, SANDERS & DEMPSEY LLP

14<sup>TH</sup> Floor

8000 Towers Crescent Drive

Tysons Corner, Virginia 22182-2700

Telephone: 703-720-7800

Fax: 703-720-7802

APN:kmp